Claims:

1. A method for safe processing of externally generated (e.g. from the Internet) executable code and the secure downloading of information from external sources (such as the Internet), such that no contamination or (other compromise) from such external executable code and/or information is experienced by the system being protected (referred to as the protected-system) by the invention (a secure communications & processing front-end signal control system), comprising the steps of;

a. inserting a secure communications & processing front-end signal control system between the protected-system and external signal sources (e.g. the Internet), such that all external signals are confined in the secure communications & processing front-end signal control system (the invention), and all external signals are processed inside the invention, whereby the protected-system is thus physically isolated (at the signal level) from potentially hostile/contaminated external signals;

b. viewing (from the protected-system) the processing of external signals taking place inside the invention (where the protected-system is a manned system, such as a workstation) by making the display subsystem of the invention safely viewable from the protected-system, whereby a simple embodiment of this step is to make the monitor (e.g. VGA/SVGA output) signal of the invention viewable on a subset of the raster display (monitor) of the protected-system;

c. allowing the protected-system to capture (and store in any desired format) the display output signals (e.g. monitor's video data stream) from the invention, whereby this

capture process results in an information-preserving-signal-transfer process with the carrier signal safely generated by the invention, while the original external signals are confined within the invention (the secure communications & processing front-end signal control system), thus eliminating any probability of any contamination or hostile signals (such as viruses (*of any type*), worms (*of any type*), cookies, false commands, or false command sequences (*for process-control and telemetry type applications*), and like signals) reaching the protected-system;

d. providing a one-way optical signal path to allow protected-system selected information (e.g. spreadsheets, programs needing updates, etc.) to be safely passed to the invention for update processing inside the invention, whereby the results of such processing (e.g. updates, downloading of program patches, etc.) is tested and evaluated within the invention, and transferred to the protected-system as defined in strep c;

e. processing external commands and external (e.g. from the Internet) requests to the protected system (where the protected-system is an unmanned/autonomous system such as a server, a process-control system, a web-site), and generating allowed command and request signals to the protected-system (based on the external command and request processing results), while confining all external signals in the invention (the secure communications & processing front-end signal control system), whereby this process insures no false or unauthorized commands (or unauthorized command sequences) and unauthorized requests reach the protected-system;

f. automatically returning the invention (the secure communications & processing front-end signal control system) to a predefined secure state (e.g. an initial state) via an

automatic system-reset/flush sequence initiated by the end of an external communication session (e.g. with the Internet), thus eliminating all external signals received by (and remaining in) the invention during that session, wherein this step results in an automatic self-cleansing of the invention, therefore eliminating the need for anti-virus software (and updates), cookies countermeasure software, filters, firewalls, and other (at best, marginally effective) InfoSec software functions, and keeping the protected-system safely physically-isolated from all external signals.

2. The method of claim 1, wherein the step of inserting includes connection of the invention (the secure communications & processing front-end signal control system) to the protected-system using a one-way link for signal traffic from the protected-system to the invention, and a one-way link from the invention to the protected-system, such that the one-way link from the invention to the protected-system is a signal path that will not propagate external signals, whereby the signal path is a waveguide incompatible with the structure of external signals;

3. The method of claim 1, wherein the protected-system's capture process can be any commercially available (or user generated) process including video capture, text retrieval, scanning, or like processes, whereby such processes are selected to optimize an application and embody a modified-read (information preserving data transform) function;

4. The method of claim 1, wherein processing external commands and external

requests is embodied as an automatic comparison type process wherein the repository of allowed commands and requests is available as a data set residing in the invention (the secure communications & processing front-end signal control system) in a write-protected area such as a CD/R disk;

5. The method of claim 2, wherein the step of inserting includes connecting the invention to the expansion-bus of the protected-system in such manner as to cause the invention to operate as a standard peripheral device to the protected system;

6. The method of claim 1, wherein the step of automatically returning to a predefined secure state is embodied as both an automatic system interrupt sequence executed at the end of an external communications session, and an operator initiated process such as a reset button, whereby the operator can reset/flush the invention at his/her discretion without reliance on the automatic system interrupt;

7. A system for safe processing of externally generated (e.g. from the Internet) executable code and the secure downloading of information from external sources (such as the Internet), such that no contamination or (other compromise) from such external executable code and/or information is experienced by the system being protected (referred to as the protected-system) by the invention (a secure communications & processing front-end signal control system), comprising;

a. a means for inserting a secure communications & processing front-end signal

control system between the protected-system and external signal sources (e.g. the Internet), such that all external signals are confined in the secure communications & processing front-end signal control system (the invention), and all external signals are processed inside the invention, whereby the protected-system is thus physically isolated (at the signal level) from potentially hostile/contaminated external signals;

b. a means for viewing (from the protected-system) the processing of external signals taking place inside the invention (where the protected-system is a manned system, such as a workstation) by making the display subsystem of the invention safely viewable from the protected-system, whereby a simple embodiment of this step is to make the monitor (e.g. VGA/SVGA output) signal of the invention viewable on a subset of the raster display (monitor) of the protected-system;

c. a means for allowing the protected-system to capture (and store in any desired format) the display output signals (e.g. monitor's video data stream) from the invention, whereby this capture process results in an information-preserving-signal-transfer process with the carrier signal safely generated by the invention, while the original external signals are confined within the invention (the secure communications & processing front-end signal control system), thus eliminating any probability of any contamination or hostile signals (such as viruses (*of any type*), worms (*of any type*), cookies, false commands, or false command sequences (*for process-control and telemetry type applications*), and like signals) reaching the protected-system;

d. a means for providing a one-way optical signal path to allow protected-system selected information (e.g. spreadsheets, programs needing updates, etc.) to be safely

passed to the invention for update processing inside the invention, whereby the results of such processing (e.g. updates, downloading of program patches, etc.) is tested and evaluated within the invention, and transferred to the protected-system as defined in step c;

e. a means for processing external commands and external (e.g. from the Internet) requests to the protected system (where the protected-system is an unmanned/autonomous system such as a server, a process-control system, a web-site), and generating allowed command and request signals to the protected-system (based on the external command and request processing results), while confining all external signals in the invention (the secure communications & processing front-end signal control system), whereby this process insures no false or unauthorized commands (or unauthorized command sequences) and unauthorized requests reach the protected-system;

f. a means for automatically returning the invention (the secure communications & processing front-end signal control system) to a predefined secure state (e.g. an initial state) via an automatic system-reset/flush sequence initiated by the end of an external communication session (e.g. with the Internet), thus eliminating all external signals received by (and remaining in) the invention during that session, wherein this step results in an automatic self-cleansing of the invention, therefore eliminating the need for anti-virus software (and updates), cookies countermeasure software, filters, firewalls, and other (at best, marginally effective) InfoSec software functions, and keeping the protected-system safely physically-isolated from all external signals.

8. The system of claim 7, wherein the invention is embodied as a device selected from a group of computer hardware devices, including single board computers, modified single board computers, embedded microprocessors, embedded microcontrollers, personal computers, portable/laptop computer systems, mainframe computers, palmtop computers, network computer systems, and like devices;

9. The system of claim 7, including means for identifying a protected system for authorized access to the intermediate domain device of the invention (the secure communications & processing front-end signal control system);

10. The system of claim 7, wherein said intermediate domain device of the invention is selected from a group of computer hardware devices, including single board computers, embedded microprocessors, embedded microcontrollers, personal computers, handheld units, portable/laptop computer systems, mainframe computers and network computer systems;

11. The system of claim 7, wherein said means for viewing, means for allowing, means for providing a one-way link, means for processing, and means for automatically returning to a predefined secure state are embodied as a system inserted in the expansion-bus of the protected-system;

12. The system of claim 11, wherein the invention (a secure communications & processing front-end signal control system) is embodied as a single-board-computer

modified to operate as a peripheral device to the protected system, while residing on the expansion-bus of the protected-system, whereby the size and performance of the invention are scalable (up/down) for optimal application-specific operation;

13. The system of claim 12, including a plurality of the invention (a secure communications & processing front-end signal control system);

14. The system of claim 12, wherein a network of systems, each protected by an embodiment of the invention (a secure communications & processing front-end signal control system), form an automatic self-cleansing network via the embodiment of the means (of each invention) to automatically return to a predefined secure state, whereby the plurality of the invention forms a secure network overlay for the network of protected-systems;

15. The plurality of claim 14, wherein each member of the plurality (of the invention) has a DIN (Device Identification Number) authentication capability, whereby each member of the plurality can authenticate (at the signal-level) all other members of the plurality, thus isolating unauthorized (i.e. *non* DIN-authentication-capable) devices, if any, of the plurality;

16. The system of claim 7, wherein the means for processing commands and requests includes a user/operator transmit-control filter function, such that no data units

(such as e-mail packets) can be transmitted from the invention to external sites (such as the Internet) without direct user action/approval, whereby such approval is embodied as an affirmative response to a system-level transmit request by the invention (a secure communications & processing front-end signal control system).

17. The method of claim 1 wherein the processing step includes selecting an internal data set that is to react with the initial data set, transferring the internal data set to the intermediate domain device and thereafter processing the initial and internal data sets within the intermediate domain device thus confining undesirable data to the intermediate domain device and obtaining the second data set;

18. The method of claim 17 including the additional step of filtering the selected internal data set for authorized transfer to the intermediate domain device;

19. The system of claim 7 including means for filtering information to be transmitted to the invention (from the protected system) to thereby prevent unauthorized release of information from the protected system, whereby this filtering step can involve inputs from other invention devices (secure communications & processing front-end signal control systems) in a network, thus implementing a "2-person rule" type filter function in a network of invention devices;

20. The system of claim 7 wherein said intermediate domain device is selected

from a group of computer hardware devices, including single board computers, modified single board computers, embedded microprocessors, embedded microcontrollers, personal computers, webtv units, portable/laptop computer systems, mainframe computers, network computer systems, network of computers, and a plurality of such devices, whereby a modified single board computer devise includes a "commercial of the shelf" (COTS) single board computer device modified to include an embedded "non-transparent" bus-bridge device which permits the single board computer to operate as an add-in card to the bus;

21. The system of claim 7 including means for identifying a protected system for authorized access to the intermediate domain device;

22. The system of claim 7 in which said means for connecting, means for processing, and extracting and means for passing, means for purging, means for resetting are mounted to a bus of the protected system;

23. The system of claim 22 including a plurality of intermediate domain devices;

24. The system of claim 7 including a plurality of intermediate domain computer hardware devices, and means for identifying authorized intermediate domain computer hardware devices in a network;

25. The system of claim 24 wherein the means for identifying includes a DIN

(Device Identification Number) authentication capability, and a data set labeling capability;

26. The system of claim 25 wherein the DIN authentication capability and the data set labeling capability includes the means to generate, transceive, and process patterns of information (representing DIN's or labeled data sets) that appear as noise to unauthorized receivers, and cannot be correctly generated by unauthorized transmitters, whereby encypherment is an example of such means, and would thus include (application specific) encypherment key management;

27. The system of claim 26 wherein the means to transceive can operate in the framework of any telecommunication medium including IP data packets, physical waveguides (e.g. air, optic fiber, wire) and the means for processing includes adaptive processing capability, such that some limitations of binary computation are removed from the process;

28. The system of claim 7, wherein a plurality of such systems (due to the means for purging, and means for resetting) includes the means to intrinsically and automatically eliminate any contamination from the plurality, wherein the plurality includes networks of the system;

29. The system of claim 7, wherein the means for connecting includes an initialization process for the system, such that the system begins and ends an active

period(such as an external session), in a contamination-free state;

30. The system of claim 7, wherein the means for connecting and means for processing include the capability to control the flow (based on parameters including type, rate, labels) of signal traffic (including data sets) to and from the system, based on the DIN of the system and the label of the signal traffic, wherein the DIN of a system is considered a label of that system;

31. The system of claim 30, wherein the means for connecting and means for processing includes the capability to derive the point of origin of signal traffic received by the system;

32. The system of claim 31, wherein the means for connecting and means for processing includes the means to generate system status information, transmit such information to a like systems (in a network of like systems);

33. The system of claim 32, wherein the means for connecting and means for processing includes the means to receive device status from like systems (in a network of like systems), process such information, and take action (based on results of such processing) relative to the network of like systems;

34. The system of claim 7, wherein the means for connecting includes an

expansion-bus interface module (EBIM), when the intermediate domain device is embodied as a single board computer type device, such that the EBIM permits the intermediate domain device to interface (as an add-in card) with the expansion-bus o f the host-protected system, whereby the EBIM can be embodied as an expansion-bus bridge device;

35. The system of claim 7, wherein the protected system is a component of the system defined in claim 7;

36. The system of claim 7, wherein the means for processing and means for securely passing includes a means for secure processing and execution of "executable code" received from an external data set source and secure passing of the results (of such processing and execution) to the protected system;

37. The system of claim 31, wherein the means for connecting and means for processing includes the capability to authenticate the contents of signal traffic received by the system, when said received signal traffic has been appropriately processed (for transmission) by the transmitting system;

38. The system of claim 16, wherein the means for connecting and means for processing includes the capability to process data-sets (that are to be transmitted to external destinations), in such manner as to permit authentication of the contents of such data-sets upon arrival at the destination, whereby the destination has a compatible

authentication processing capability;

39. The system of claim 36, wherein the means for securely passing includes the means for securely transferring (to the protected domain) data units resulting from the processing of external executable programs, whereby such external executable programs may contain contaminates hostile to the protected domain;

40. The system of claim 38, wherein data sets with contents that cannot be authenticated are deleted from the system with no information transfer to the protected domain, thereby preventing the protected domain from incurring faults/errors or other compromise that could be induced by information from faulty/erroneous external signals;

41. The system of claim 7, wherein the protected system is a router, switch, hub, or like network device, wherein the means for processing and the means for securely passing include the capability to analyze both incoming and outgoing data units so as to identify improper data units, delete such improper (as determined by specific application parameters) data units, and control the flow of data units to and from the protected system, whereby adverse operational impact on the protected system is minimized;

42. The system of claim 41, wherein means for processing and means for securely passing include the capability to generate status information, tranceive such status information with adjacent like-devices (e.g. in a network), and analyze such status

information, for the purpose of maintaining optimal (as defined by specific applications) data unit flow control;

43. The system of claim 42, wherein the means for connecting, means for processing, and means for securely passing include the capability to monitor and determine the rate of incoming data-units and control that rate, such that the rate of incoming data-units does not exceed a specific threshold;

44. The system of claim 43, wherein the means for connecting, means for processing, and means for securely passing include the means to control the transmission of data-units from the system, to external systems, in such manner that individual data-units are transmitted only after specific control authorization from a designated source, whereby such features can be used as countermeasures to denial-of-service (DoS) type attacks and congestion type conditions originating from external links;

45. The system of claim 44, wherein the means for connecting, means for processing, and means for securely passing include the means to buffer and decontaminate incoming multimedia data streams, to maximize quality-of-service (QoS)/signal-integrity parameters for those data streams and make the resultant data stream available for "protected system" use, thus acting as a local multimedia "server" to its protected system, whereby the protected-system "client" accesses the system (in a client/server mode) thereby countering signal quality degradation encountered over

external links to the system.